

TS. LÊ ĐẮC NHƯỜNG

AN TOÀN DỮ LIỆU

MÃ HÓA BẢO MẬT THÔNG TIN,
AN NINH CƠ SỞ DỮ LIỆU VÀ AN NINH MẠNG

TS. LÊ ĐẮC NHƯỜNG

AN TOÀN DỮ LIỆU

- MÃ HÓA BẢO MẬT THÔNG TIN
- AN NINH CƠ SỞ DỮ LIỆU
- VÀ AN NINH MẠNG



NHÀ XUẤT BẢN ĐẠI HỌC QUỐC GIA HÀ NỘI



Mục lục

Chương 1. Tổng quan về an toàn dữ liệu	11
1.1 Sơ lược lịch sử về khoa học mật mã	11
1.2 Sự cần thiết phải đảm bảo an toàn dữ liệu	14
1.2.1 Những nguy cơ tiềm ẩn mất an toàn dữ liệu	14
1.2.2 Các bài toán về an toàn dữ liệu	15
1.3 Mật mã và tính an toàn của các hệ mã	16
1.3.1 Một số thuật ngữ	16
1.3.2 Định nghĩa hệ mật mã	16
1.3.3 Những yêu cầu đối với hệ mật mã	17
1.3.4 Phân loại phương pháp mã hóa	17
1.3.5 Thám mã và tính an toàn của hệ mật mã	18
1.4 Cơ sở toán học	20
1.4.1 Số nguyên tố	20
1.4.2 Phần tử nghịch đảo	22
1.4.3 Phương trình đồng dư tuyến tính	24
1.4.4 Định lý số dư Trung hoa	25
1.4.5 Bài toán Logarit rời rạc	25
1.4.6 Phân tích thành thừa số nguyên tố	26
1.4.7 Thuật toán tính $y = x^k \bmod N$	27

1.4.8	Bài toán về tổng các tập con	27
1.4.9	Hàm một phía và hàm cửa sập một phía	28
1.5	Câu hỏi, bài tập và thực hành	29

Chương 2. Các hệ mã hóa dữ liệu 31

2.1	Nguyên tắc chung của các hệ mã hóa	31
2.2	Các hệ mã hóa khóa cổ điển	32
2.2.1	Mã dịch vòng	32
2.2.2	Mã thay thế	33
2.2.3	Mã Affine	34
2.2.4	Mã Vigenère	34
2.2.5	Mã Hill	35
2.2.6	Mã hoán vị	36
2.2.7	Mã Playfair	37
2.2.8	Mã Rail Fence	38
2.3	Các hệ mã hóa khóa hiện đại	38
2.3.1	Mã DES-Data Encryption System	38
2.3.2	Mã AES-Advanced Encryption Standard	47
2.4	Hệ mã khoá công khai	53
2.4.1	Hệ mã hóa RSA	54
2.4.2	Hệ mã hóa Rabin	58
2.4.3	Hệ mã hóa Elgamal	59
2.4.4	Hệ mã hóa Merkle-Hellman	60
2.4.5	Hệ mã hóa McEliece	61
2.4.6	Hệ mã hóa trên đường cong Elliptic	63
2.4.7	Mật mã hạng nhẹ (<i>Lightweight Cryptography</i>)	66
2.5	Câu hỏi, bài tập và thực hành	67

Chương 3. An toàn trong giao dịch điện tử 71

3.1	Hàm băm	71
3.1.1	Hàm băm Chaum-van Heijst-Pfitzmann	73
3.1.2	Hàm băm MD5	73
3.1.3	Hàm băm SHA-1	74
3.1.4	Phân tích, đánh giá hàm băm MD5 và SHA-1	76
3.2	Chữ ký số	77
3.2.1	Định nghĩa và phân loại sơ đồ ký	78
3.2.2	Sơ đồ ký RSA	79
3.2.3	Sơ đồ chữ ký Rabin	81
3.2.4	Sơ đồ chữ ký ElGamal	81
3.2.5	Sơ đồ chữ ký Schnorr	82
3.2.6	Chuẩn chữ ký số DSS	83

3.2.7	Chữ ký số ECC	84
3.2.8	Chữ ký mù Chaum	85
3.2.9	Tấn công chữ ký số	86
3.3	Chia sẻ bí mật và phân phối khoá	86
3.3.1	Chia sẻ bí mật Shamir	86
3.3.2	Phân phối khoá Bloom	89
3.3.3	Phân phối khoá Kerberos	89
3.3.4	Phân phối khoá Diffie-Hellman	90
3.4	Sơ đồ định danh và xác thực danh tính	92
3.4.1	Sơ đồ định danh Schnorr	93
3.4.2	Sơ đồ định danh Okamoto	94
3.5	Một số ứng dụng trong thương mại điện tử	95
3.5.1	Chứng chỉ số	95
3.5.2	Thanh toán điện tử	97
3.5.3	Tiền điện tử	99
3.5.4	Hợp đồng điện tử	100
3.5.5	Đấu giá điện tử	102
3.5.6	Bỏ phiếu điện tử	103
3.6	Câu hỏi, bài tập và thực hành	105
Chương 4. An ninh cơ sở dữ liệu		107
4.1	Tổng quan về an ninh cơ sở dữ liệu	107
4.2	Cơ chế kiểm soát và chính sách an toàn dữ liệu	112
4.2.1	Cơ chế kiểm soát luồng	112
4.2.2	Cơ chế kiểm soát suy diễn	112
4.2.3	Cơ chế kiểm soát truy nhập	112
4.2.4	Chính sách đặc quyền	114
4.3	Các quy tắc trao quyền, xác thực, cấp quyền	115
4.3.1	Chính sách quản lý quyền	115
4.3.2	Các quy tắc trao quyền	115
4.3.3	Các phương thức xác thực và định danh	120
4.4	An toàn hệ quản trị cơ sở dữ liệu	123
4.4.1	Cơ chế an toàn trong các hệ quản trị cơ sở dữ liệu	124
4.4.2	Các cơ chế toàn vẹn trong các hệ quản trị cơ sở dữ liệu	125
4.4.3	Mô hình cấp quyền System R	126
4.4.4	Các kiến trúc của hệ quản trị cơ sở dữ liệu an toàn	127
4.4.5	Phát hiện xâm nhập trái phép cơ sở dữ liệu	130
4.4.6	Kiểm toán cơ sở dữ liệu	133
4.4.7	Kiểm toán cơ sở dữ liệu trên SQL Server	138

4.4.8	Kiểm toán cơ sở dữ liệu trên Oracle	140
4.4.9	Thiết kế các cơ sở dữ liệu an toàn	143
4.5	Câu hỏi, bài tập và thực hành	145

Chương 5. An ninh mạng 147

5.1	Tổng quan về an ninh mạng	147
5.1.1	Các vấn đề trong an ninh mạng	147
5.1.2	Quy trình và mô hình tấn công mạng	149
5.1.3	Các mức an toàn bảo mật hệ thống mạng	151
5.1.4	Các loại lỗ hổng bảo mật	152
5.2	Các hình thức tấn công mạng phổ biến	153
5.2.1	Tấn công thăm dò	153
5.2.2	Tấn công truy nhập	154
5.2.3	Tấn công biến đổi thông tin	155
5.2.4	Tấn công chiếm quyền điều khiển	156
5.2.5	Tấn công từ chối dịch vụ và biện pháp phòng chống	156
5.2.6	Tấn công khước từ thống kê	160
5.2.7	Tấn công tràn bộ đệm	160
5.2.8	Tấn công Back Door	162
5.2.9	Tấn công giả mạo	162
5.2.10	Tấn công lặp lại	163
5.2.11	Tấn công Brute Force	164
5.3	An toàn dịch vụ web	164
5.3.1	Giao thức http/https	164
5.3.2	Giao thức SSL/TSL	165
5.3.3	SQL Injection	171
5.3.4	Cross Site Scripting	173
5.3.5	Tường lửa	174
5.4	Bảo mật trong mạng không dây	176
5.4.1	Quy trình bắt tay 4 bước trong kết nối Wifi	177
5.4.2	Giao thức WEP	178
5.4.3	Giao thức bảo toàn dữ liệu với khoá theo thời gian TKIP	180
5.4.4	Giao thức WPA	181
5.4.5	Giao thức WPA2	182
5.4.6	Giao thức WPA3	184
5.4.7	Mạng riêng ảo VPN	184
5.5	Câu hỏi, bài tập và thực hành	185

Chương 6. Hệ thống câu hỏi trắc nghiệm 187
Chương 7. Cài đặt các hệ mã hóa 209

7.1	Cài đặt hệ mã hóa dịch vòng	209
7.2	Cài đặt hệ mã hóa thay thế	209
7.3	Cài đặt hệ mã hóa Affine	210
7.4	Cài đặt hệ mã hóa Vignere	211
7.5	Cài đặt hệ mã hóa hoán vị	212
7.6	Cài đặt hệ mã hóa Hill	212
7.7	Cài đặt hệ mã hóa Playfair	214
7.8	Cài đặt hệ mã hóa Rail Fence	216
7.9	Cài đặt hệ mã hóa DES	217
7.10	Cài đặt hệ mã hóa AES	219
7.11	Cài đặt hệ mã hóa RSA	236
7.12	Cài đặt hệ mã hóa Rabin	237
7.13	Cài đặt chữ ký số ECC	238
7.14	Cài đặt chữ ký số RSA	244
7.15	Cài đặt hệ mã hóa và chữ ký số Elgamal	245
7.16	Cài đặt chữ ký số Schnorr	250
7.17	Cài đặt hàm băm SHA	254
7.18	Cài đặt hàm băm MD5	257



AN TOÀN DỮ LIỆU

- MÃ HÓA BẢO MẬT THÔNG TIN
- AN NINH CƠ SỞ DỮ LIỆU
- VÀ AN NINH MẠNG



Giá: 130.000đ